

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

SITNET LLC,

Plaintiff,

v.

META PLATFORMS, INC.,

Defendant.

1:23-CV-06389 (AS)

**ORDER RE:**  
**DISCOVERY OF**  
**ELECTRONICALLY STORED**  
**INFORMATION**

ARUN SUBRAMANIAN, U.S.D.J.

Plaintiff SitNet, LLC (“SitNet” or “Plaintiff”) and Defendant Meta Platforms, Inc. (“Meta” or “Defendant”) (collectively, “parties”), hereby agree that the following procedures shall govern the discovery of electronically stored information and production of documents in this matter.

**1. PURPOSE**

This Order will govern discovery of electronically stored information (“ESI”) (“eDiscovery”) in this case as a supplement to the Federal Rules of Civil Procedure (hereafter, “Rules” or “Rule”) and any other applicable orders and rules.

**2. COOPERATION AND PROPORTIONALITY**

The parties are aware of the importance of cooperation and commit to cooperate in good faith throughout the matter to promote the “just, speedy, and inexpensive determination” of this action, as required by Rule 1. The parties’ cooperation includes propounding reasonably particular discovery requests, identifying appropriate limits to eDiscovery, including limits on custodians, identifying relevant and discoverable ESI, establishing time periods for eDiscovery and other parameters to limit and guide preservation and eDiscovery issues. The failure of counsel or the parties to cooperate in facilitating and reasonably limiting eDiscovery requests

and responses will be considered in cost-shifting determinations. The parties agree to use reasonable, good faith, and proportional efforts to preserve, identify, and produce relevant and discoverable information consistent with Rule 26(b)(1).

### **3. LIAISON**

Each party shall designate or make available, an individual or individuals as eDiscovery Liaison(s) who must:

- (a) be prepared to meet and confer on eDiscovery-related matters and to participate in eDiscovery dispute resolution;
- (b) be knowledgeable about the party's eDiscovery efforts;
- (c) be, or have reasonable access to those who are, familiar with the party's electronic systems and capabilities in order to explain those systems and answer relevant questions; and
- (d) be, or have reasonable access to those who are, knowledgeable about the technical aspects of eDiscovery, including electronic document storage, organization, and format issues, and relevant information retrieval technology, including search methodology.

### **4. PRESERVATION**

Each party is responsible for taking reasonable and proportionate steps to preserve relevant and discoverable ESI within its possession, custody or control. The parties have discussed their preservation obligations and needs and agree that relevant and proportionate ESI will be preserved. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

- (a) Parties will preserve non-duplicative, discoverable information currently in their possession, custody, or control; however, parties are not required to modify, on a going-forward basis, the procedures used by them in the usual course of business to back up and archive data.
- (b) Subject to and without waiving any protection described in Section 4(a) above, the parties agree that:
  - (1) The parties have discussed the sources and types of relevant ESI they believe should be preserved.

- (2) The parties will agree on the number of custodians per party for whom ESI will be preserved. The parties agree to meet & confer to discuss additional custodians as reasonably necessary (i.e., when specific evidence warrants expanding the initial custodian list).
- (c) The following data sources are not reasonably accessible because of undue burden or cost pursuant to Rule 26(b)(2)(B), and unwarranted extraordinary measures will not be taken to preserve ESI from these sources, which will be retained pursuant to standard business processes, but not otherwise preserved, searched, reviewed, or produced, unless ordered by the Court upon a motion of a party:
  - (1) backup systems and/or tapes used for disaster recovery; and
  - (2) systems no longer in use that cannot be accessed by using systems currently in use by the party.
- (d) The following data types are not reasonably accessible because of undue burden or cost pursuant to Rule 26(b)(2)(B), and unwarranted extraordinary measures will not be taken to broadly preserve this ESI, and instead, it will be retained pursuant to standard business processes, but not otherwise preserved, searched, reviewed, or produced, unless ordered by the Court upon a motion of a party:
  - (1) Voice messages.
  - (2) Instant messages and chats that are not chronicled to an email archive system.
  - (3) Sound recordings, including, without limitation, .mp3/.mp4 and .wav files.
  - (4) Video recordings.
  - (5) Information solely contained on mobile devices that is duplicative of information available elsewhere.
- (e) In addition to the agreements above, the parties agree data from these sources (a) could contain relevant information but (b) under the proportionality factors, should not be preserved:
  - (1) Deleted, slack, fragmented, or unallocated data only accessible by forensics.
  - (2) Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.
  - (3) On-line data such as temporary internet files, history, cache, cookies, and the like.

- (4) Data in metadata fields that are frequently updated automatically, such as last-opened or last modified dates.
  - (5) Mobile device activity logs.
  - (6) Server, system, or network logs.
  - (7) Dynamic fields in databases or log files not stored or retained in the usual course of business.
  - (8) Information created or copied during the routine, good-faith performance of processes for the deployment, maintenance, retirement, and/or disposition of computer equipment by the party.
  - (9) Other forms of ESI whose preservation requires unreasonable, disproportionate, and/or non-routine, affirmative measures that are not utilized in the ordinary course of business.
- (f) The parties acknowledge that Meta Platforms, Inc. is subject to various privacy regulations and court orders that require the disposition of identifiable user data. To the extent that identifiable user data subject to routine disposition as required by privacy regulations and court orders is identified as relevant to the claims or defenses in this case, the parties will meet and confer on preservation of such information as it exists at that time, including the feasibility of such preservation and the type and import of the user data implicated.

## 5. SEARCH

The fact that a document or ESI is responsive to a search term or identified as responsive by any other technology used to identify potentially responsive Documents and ESI shall not prevent any Party from withholding such file from production on the grounds that the file is protected from disclosure by applicable privilege or work-product protection. The parties agree that in responding to an initial Rule 34 request, or earlier if appropriate, they will disclose the method or methods they are intending to employ to identify the appropriate set(s) of documents for review and production. The use of a search methodology does not relieve a party from its obligations under the Rules to produce responsive documents, and accordingly documents or ESI known to be responsive to a discovery request or otherwise subject to production or relevant to the claims or defenses shall be produced without regard to whether it was returned by any search

methodology used in accordance with this Order or otherwise agreed upon by the parties unless there is a claim of privilege.

- (a) Search Terms. Where a producing party determines it will use search terms to cull potentially responsive ESI, the producing party will disclose the search terms to the receiving party. If, after disclosure of the producing party's search terms, a requesting party believes in good faith that the producing party's search terms would result in deficiencies in the production, the requesting party may suggest a reasonable number of additional search terms. The parties shall resolve any disputes regarding the application of search terms by following the discovery-disputes procedure set forth in the Court's Individual Practices in Civil Cases. If a producing party asserts that any search term proposed by the receiving party is overbroad, not sufficiently targeted, results in too many hits, or makes any other argument that the proposed search term is unduly burdensome or not proportional to the needs of the case, they shall produce a hit report to support this assertion.
  1. Hit Reports. A hit report shall contain the following with respect to each proposed or modified search term in the collection:
    - (i) The number of documents with hits for that term;
    - (ii) The number of unique documents, i.e., documents which do not have hits for any other term, for that term;
    - (iii) The number of family members requiring review in connection with all documents with hits; and
- (b) Technology Assisted Review. A party may use technology assisted review ("TAR") or similar advanced analytics to filter out or exclude non-responsive documents.<sup>1</sup> A receiving party may request the following information about a producing party's use of TAR or similar advanced analytics limited to the following: (1) the custodians and data sources against which TAR or advanced analytics will be run; (2) the TAR or advanced analytics tool being used and vendor; and (3) the measure(s) used to validate the results of the TAR methodology or similar advanced analytics.
- (c) Other Review Procedures. Nothing in this Order may be construed or interpreted as precluding a producing party from performing a responsiveness review to determine if documents (1) captured by search terms or (2) identified as potentially responsive through TAR are in fact relevant to the requesting party's discovery requests. Similarly, nothing may be construed or interpreted as precluding a producing party from performing, by any means, a privilege review of documents determined to be relevant. Further, nothing in this Order requires the production of documents captured by any

---

<sup>1</sup> A producing party need not disclose whether it is using TAR, Continuous Active Learning ("CAL"), or any other predictive coding to prioritize the review of documents collected.

search term that are irrelevant to the requesting party's request, privileged, or otherwise protected from disclosure.

- (d) System Files and Executables. Each party will use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. For example, Hash values may be filtered out during this process using the National Software Reference Library ("NSRL") NIST hash set list.
- (e) De-Duplication. Each party is required to produce only a single copy of a responsive document and each party may de-duplicate responsive ESI (e.g., based on MD5 hash function) across custodians. The hash value will be generated at a family level.
- (f) Email Threading. Where multiple email messages are part of a single chain or "thread," a party is only required to produce the most inclusive message ("Last In Time Email") and need not produce earlier, less inclusive email messages or "thread members" that are fully contained, including attachments and including identical senders and recipients, within the Last In Time Email. Only email messages for which the parent document and all attachments are contained in the Last In Time Email will be considered less inclusive email messages that need not be produced.
- (g) Source code. Other than Section 6, no other provision of this Order affects any inspection of source code that is responsive to a discovery request consistent with the Protective Order governing this case.
- (h) On-site inspection. On-site inspection will not be permitted absent a demonstration by the requesting party of specific need and good cause or by agreement of the parties.

## 6. SOURCE CODE INSPECTION AND PRODUCTION

The parties agree that the following procedures govern source-code inspection and production.

- (a) Any source code produced in discovery shall be made available for inspection, in a format allowing it to be reasonably reviewed and searched, during normal business hours (9:00 am to 5:00 pm local time) or at other mutually agreeable times, at an office of the producing party's counsel selected by the producing party or another mutually agreed upon location. The computer containing source code (the "Source Code Computer") will be made available upon reasonable notice to the producing party, which shall not be less than five (5) business days in advance of the requested inspection. The name(s) of the person(s) who review the source code will be provided to Meta as part of this notice. The producing party will have seven (7) business days from receipt of the notice to object to providing access to any person(s) identified in the notice, pursuant to the procedures set forth in the Protective Order entered in this case. The source code shall be made available for inspection on a secured computer in a room without Internet access or network access to other computers, and the receiving party shall not copy, remove, photograph, or otherwise transfer or image any portion of the source code onto any recordable media or

recordable device. The producing party may visually monitor the activities of the receiving party's representatives during any source code review, but only to ensure that there is no unauthorized recording, copying, or transmission of the source code. All persons viewing source code shall sign a log on each day they view source code. The producing party will maintain a log that includes the names of persons who enter the room to view the source code and when they enter and depart. All persons viewing source code shall sign the log on each day they view source code.

- (b) The receiving party may request paper copies of limited portions of source code that are reasonably necessary to attach to filings, pleadings, expert reports, or other papers, or for use as an exhibit at deposition or trial, but shall not request paper copies for the purposes of reviewing the source code other than electronically as set forth in paragraph (a) in the first instance. Using the software available on the Source Code Computer, the receiving party shall create PDFs of the printed copies the receiving party is requesting and save them in a folder on the desktop named "Print Requests" with a subfolder identifying the date of the request. The PDF printouts must include identifying information including the full file path and file name, page number, line numbers, and date. The request for printed source code shall be served via an email request identifying the subfolders of the "Print Requests" folder that the receiving party is requesting. Within five (5) business days of such request, the producing party will use its best efforts to provide three copies of all such source code on watermarked or colored paper, including bates numbers and the label "Highly Confidential – Source Code." If the request is served after 5:00 p.m. Pacific Time, it shall be deemed served the following business day. The receiving party may not request more than 30 consecutive pages, or an aggregate of more than 300 pages, of source code during the duration of the case without requesting written approval of the producing party to exceed these limits, which the producing party shall not unreasonably deny. The producing party may challenge the amount of source code requested in hard copy form pursuant to the dispute resolution procedure set forth in Paragraph 15 of the Protective Order.
- (c) The receiving party shall maintain a log of all paper copies of the source code. The log shall include the names of the reviewers and/or recipients of paper copies and locations where the paper copies are stored. Upon seven (7) day's advance notice to the receiving party by the producing party, the receiving party shall provide a copy of this log to the producing party. The receiving party shall maintain all paper copies of any printed portions of the source code in a secured, locked area. The receiving party shall not create any electronic or other images of the paper copies and shall not convert any of the information contained in the paper copies into any electronic format. The receiving party shall only request additional paper copies if such additional copies are (1) necessary to attach to court filings, pleadings, or other papers (including a testifying expert's expert report), (2) necessary for deposition, or (3) necessary for trial. The receiving party shall not request paper copies for the purposes of reviewing the source code other than electronically as set forth in paragraph (c) in the first instance. To the extent a deposition is likely to involve material designated Highly Confidential – Source Code, the party taking the deposition shall provide at least seven (7) days' written notice.



- (d) The producing party shall install tools that are sufficient for viewing the Source Code produced for inspection on the Source Code Computer. The Parties shall meet and confer regarding any additional tools that the Receiving Party requests be added. To the extent additional tools are provided at the Request of the Receiving Party, the Receiving Party is responsible for securing the appropriate licenses for such software tools.
- (e) No recordable media or recordable devices, including, without limitation, sound recorders, computers, cellular telephones, peripheral equipment, cameras, CDs, DVDs, or drives of any kind, shall be permitted into the source code review room.
- (f) The receiving party's Outside Counsel and/or experts/consultants shall be entitled to take hand-written notes relating to the source code but may not copy the source code into the notes and may not take such notes electronically on the Source Code Computer itself or any other computer. Such notes must be treated and labeled as Highly Confidential – Source Code information under the Protective Order.
- (g) The receiving party's outside counsel and any person receiving a copy of any source code shall maintain and store any paper copies of the source code at their offices in a manner that prevents duplication of or unauthorized access to the source code, including, without limitation, storing the source code in a locked room or cabinet at all times when it is not in use.
- (h) Upon request from the receiving party at least seven (7) days in advance, the producing party shall make a Source Code Computer available for use during deposition by persons authorized to have access to such materials.

## **7. PRODUCTION FORMATS**

The parties agree to produce documents in the formats described in Appendix 1 to this Order. If particular documents warrant a different format, the parties will cooperate to arrange for the mutually acceptable production of such documents. The parties agree, to the extent practicable, not to materially degrade the searchability of documents as part of the document production process.

## **8. PHASING**

When a party propounds discovery requests pursuant to Rule 34, the parties agree to phase the production of ESI. Following the initial production, the parties will continue to prioritize the order of subsequent productions.



## 9. DOCUMENTS PROTECTED FROM DISCOVERY

- (a) The parties have submitted, and the Court has entered, a separate Protective Order that governs the production of documents protected from discovery.
- (b) Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Rules 26(b)(3)(A) and (B).
- (c) Communications involving or work product associated with inside or outside counsel for the parties related to this case that post-date the filing of the complaint need not be placed on a privilege log.
- (d) The Parties agree to log only the Last In Time Emails in a thread and need not log earlier, less inclusive email messages or “thread members” that are fully contained within the Last In Time Email. Attachments to emails shall be logged as separate documents on the log, with family relationships identified.
- (e) Privilege logs will be produced on a rolling basis within 30 days after each rolling production for documents that would have been included in that production had they not been withheld on the basis of privilege.
- (f) Each Party’s Privilege Log must provide the objective metadata listed below (to the extent it is reasonably available and does not reflect privileged or protected information) and the privilege or protection being asserted. Privilege logs will be produced in an Excel or spreadsheet format that allows the Receiving Party to search and sort all columns and entries of the privilege log. The party need not include a more detailed description of the document or the factual basis for the assertion of a privilege or protection unless the disclosure of that additional information is necessary to resolve a dispute.
  - (i) Bates Number or other unique identifier
  - (ii) Author
  - (iii) Subject
  - (iv) Title
  - (v) Attachment Name
  - (vi) File Name
  - (vii) Sender From/To
  - (viii) Recipient/To
  - (ix) CC
  - (x) BCC

- (xi) Sent Date/Time
  - (xii) Created Date/Time
  - (xiii) Date/Time Last Modified
  - (xiv) Family relationship (e.g., identifying parent emails and attachments)
  - (xv) File Extension
  - (xvi) Hash Value
  - (xvii) Privilege asserted
- (g) The privilege log will clearly identify (a) any attorneys on the privilege log using an asterisk or other agreed-upon method, and (b) any third party (along with the name of the third-party business, and the job title and/or role of the third party).
- (h) Following the receipt of a privilege log or documents that have been redacted for privilege, a receiving party may challenge for good cause, in writing, any entry on the log. The Producing party shall respond to such reasonable requests (in number or volume) either by producing the challenged document or providing an explanation as to why the challenge lacks merit within 21 days. If no agreement is reached, the receiving party may seek an order from the Court compelling production of the information. The receiving party should follow the procedures in Paragraph 5 of the Court's Individual Practices in Civil Cases.
- (i) Nothing in this Order requires disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity. The parties do not waive any objections to the production, discoverability, admissibility, or confidentiality of documents and ESI.

## **10. MODIFICATION**

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

**SO STIPULATED AND AGREED.**

Respectfully submitted,

/s/ John Cook

BARCLAY DAMON LLP  
Douglas J. Nash  
John D. Cook  
Denis J. Sullivan  
Barclay Damon LLP  
Barclay Damon Tower  
125 East Jefferson Street  
Syracuse, New York 13202  
(315) 425-2700  
dnash@barclaydamon.com  
jcook@barclaydamon.com  
dsullivan@barclaydamon.com

Naresh K. Kannan  
80 State Street  
Albany, NY 12207  
nkannan@barclaydamon.com

DiCELLO LEVITT LLC  
Greg G. Gutzler  
485 Lexington Avenue  
New York, NY 10017  
ggutzler@dicellolevitt.com

David L. Hecht  
Hecht Partners LLP  
125 Park Avenue, 25th Floor  
New York, New York 10017  
(212) 851-6821  
dhecht@hechtpartners.com

*Attorneys for Plaintiff SitNet LLC*

Dated: April 12, 2024

**SO ORDERED**

Dated: April 16, 2024  
New York, New York

/s/ Kathryn Bi

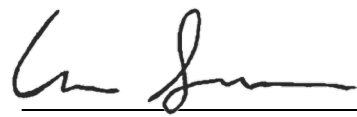
DAVIS POLK & WARDWELL LLP  
Dana M. Seshens  
Kathryn Bi  
450 Lexington Avenue  
New York, NY 10017  
Telephone: (212) 450-4000  
Facsimile: (212) 701-5800  
dana.seshens@davispolk.com  
kathryn.bi@davispolk.com

– and –

Ashok Ramani (*pro hac vice*)  
1600 El Camino Real  
Menlo Park, CA 94025  
ashok.ramani@davispolk.com

*Attorneys for Defendant Meta  
Platforms, Inc.*

Dated: April 12, 2024

  
ARUN SUBRAMANIAN  
United States District Judge

## APPENDIX 1: PRODUCTION FORMAT

**1. Production Components.** Except as otherwise provided below, ESI shall be produced in accordance with the following specifications:

- (a) an ASCII (or UTF8) delimited data file (.DAT) using standard delimiters;
- (b) an image load file (.OPT) that can be loaded into commercially acceptable production software (*e.g.* Concordance or Relativity);
- (c) TIFF images;
- (d) and document level .TXT files for all documents containing extracted full text or OCR text.
- (e) Parent-child relationships will be maintained in production. Links within a document are not considered attachments. A receiving party may make a reasonable number of requests that a producing party collect information from links within produced documents that appear to be directed to relevant information. Agreement to such requests shall not be unreasonably withheld.

If a particular document warrants a different production format, the parties will cooperate in good faith to arrange for a mutually acceptable production format.

**2. Production Media and Access Controls.** Documents shall be encrypted and produced through electronic means, such as secure file sharing methods (*e.g.* FTP), or on a CD, DVD, flash drive or external hard drive (“Production Media”). Each piece of Production Media shall identify a production number corresponding to the production volume (*e.g.* “VOL001”). Each piece of Production Media shall also identify: (a) the case caption; (b) the following label: “This media contains material subject to Court Ordered security measures”; (c) the producing party’s name; (d) the production date; and (e) the Bates Number range of the materials contained on the Production Media.

Nothing in this Order will preclude or impair any and all protections provided the parties by any Protective Order(s) agreed and entered into by the parties. Any data produced by

the producing party must be protected in transit, in use, and at rest by all in receipt of such data. Parties will use best efforts to avoid the unnecessary copying or transmittal of produced documents. Any copies made of produced data must be kept on media or hardware employing whole-disk or folder level encryption or otherwise secured on information systems and networks in a manner consistent with the best practices for data protection. If questions arise, parties will meet and confer to ensure security concerns are addressed prior to the exchange of any documents.

3. **Data Load Files/Image Load Files.** Each TIFF in a production must be referenced in the corresponding image load file. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the image load file(s) in the production. The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. All images must be assigned a unique Bates number that is sequential within a given document and across the production sets. The Bates Numbers in the image load file must match the corresponding documents' beginning Bates numbers in the data load file. The total number of documents in a production should match the total number of records in the data load file. Load files shall not vary in format or structure within a production, or from one production to another.
4. **Metadata Fields.** Each of the metadata and coding fields set forth below that are reasonably accessible at the point of collection shall be produced for each document. The parties are not obligated to populate or edit manually any of the fields below if such fields are not reasonably available when the document is collected, with the exception of the following: (a) BEGBATES, (b) ENDBATES, (c) BEGATTACH, (d) ENDATTACH, (e)

PRODVOL, (f) CUSTODIAN, (g) ALLCUSTODIAN(S), (h) CONFIDENTIALITY, (i) REDACTIONS, (j) NATIVEFILEPATH, (k) TEXTFILEPATH, (l) HASHVALUE, which should be populated by the party or the party's vendor. The parties will make reasonable efforts to ensure that metadata fields reasonably available at the time of collection will correspond directly to the information that exists in the original documents.

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family
PRODVOL	Production volume
ALLCUSTODIAN(S)	Individual(s) from whom the document was obtained and de-duplicated out during global de-duplication
ALLPARTICIPANTS	Lists all participants in lesser-included emails that, without email threading, would have been produced
CONFIDENTIALITY	Confidentiality designation assigned to document
NATIVEFILEPATH	Native File Link (Native Files only)
TEXTFILEPATH	Path to extracted text/OCR file for document
HASHVALUE	MD5 hash value of document
AUTHOR	Any value populated in the Author field of the document properties (Edoc or attachment only)
DOCDATE	Date the document was created (format: MM/DD/YYYY) (Edoc or attachment only)
DATEMODIFIED	Date when document was last modified according to filesystem information (format: MM/DD/YYYY) (Edoc or attachment only)

FILENAME	Filename of an electronic document
FILEPATH	Original path to the individual source file. Includes path up to and including internal path of containers
TITLE	Any value populated in the Title field of the document properties
DOCEXT	File extension of document pulled from the document properties
FROM	The sender of the email
TO	All recipients that were included on the “To” line of the email
CC	All recipients that were included on the “CC” line of the email
BCC	All recipients that were included on the “BCC” line of the email
DATETIMERECEIVED	Date and time email was received (format: MM/DD/YYYY HH:MM SS)
DATETIMESENT	Date and time email was sent (format: MM/DD/YYYY HH:MM SS)
EMAILSUBJECT	Subject line of email pulled from the document properties
REDACTIONS	Indicate Yes/No if document redacted
HasHiddenContent	Y if document contains hidden content <sup>2</sup> , otherwise N or empty

- 5. TIFFs.** Documents that exist only in hard copy format shall be scanned and produced as TIFFs. Documents that exist as ESI shall be converted and produced as TIFFs, except as provided below. Unless excepted below, single page, black and white, Group IV TIFFs should be provided, at least 300 dots per inch (dpi) for all documents. Each TIFF image shall be named according to a unique corresponding Bates number associated with the document. Each image shall be branded according to the Bates number and the agreed

---

<sup>2</sup> “Hidden Content” for purposes of this field shall include track changes, comments, hidden slides, hidden columns, hidden worksheets, or other hidden text.



upon confidentiality designation. Original document orientation should be maintained (i.e., portrait to portrait and landscape to landscape). Upon written request and for good cause shown, the producing party shall provide a higher quality TIFF image or the native or original file provided that the volume of documents selected for such reproduction is reasonable.

6. **Color.** The parties may make reasonable requests for color copies of documents where color is necessary to accurately interpret the document.
  
7. **Text Files.** A single multi-page text file shall be provided for each document, and the filename should match its respective TIFF filename. When possible, the text of native files should be extracted directly from the native file. Text files will not contain the redacted portions of the documents. A commercially acceptable technology for optical character recognition “OCR” shall be used for all scanned, hard copy documents and for documents with redactions.
  
8. **Native files.** The following ESI will be produced as native files:
  - (a) Spreadsheets (e.g. MS Excel) will be produced in native format unless redacted, in which instance, spreadsheets will be produced in TIFF with OCR Text Files. The receiving party may make reasonable requests to have spreadsheets produced in native format with native redactions when those spreadsheets require redactions.
  - (b) To the extent that they are produced in this action, audio, video, and multi-media files will be produced in native format.
  - (c) Presentations (e.g. MS PowerPoint) will be produced in native format.
  - (d) Word documents and PDFs with the metadata field HasHiddenContent as “Y” will be produced in native format.

Native files will be produced with a link in the NATIVEFILEPATH field, along with extracted text (where extracted text is available) and applicable metadata fields set forth in paragraph 4 above. A Bates numbered TIFF placeholder indicating that the document was provided in native format must accompany every native file.

9. **Confidentiality Designation.** Responsive documents in TIFF format will be stamped with the appropriate confidentiality designations in accordance with the Protective Order entered in this matter. Each responsive document produced in native format will have its confidentiality designation identified in the filename of the native file and indicated on its corresponding TIFF placeholder.
  
10. **Databases and Other Structured Data.** The parties shall meet and confer regarding the production format and scope of data contained in databases in order to ensure that any information produced is reasonably usable by the receiving party. If discoverable information from any Structured Data System can be produced in an already existing and reasonably available report, the Producing Party may collect and produce the data in that report format. To avoid doubt, information will be considered reasonably usable when produced in CSV format, tab-delimited text format, Microsoft Excel format, or Microsoft Access format. To the extent a party is constrained from producing responsive ESI because of a third-party license or because software necessary to view the ESI is hardware-dependent, the parties shall meet and confer to reach an agreement on alternative methods to enable the requesting party to view the ESI.